**CIDM 6340 Network Management & Information Security – Fall 2021**

**West Texas A&M University**

Homework #4

***[N.B: You can work with a team/group of MAX 5 students, but you need to submit your own Homework report. Also, please mention all group members name in the cover page]***

**Name : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Id:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Rubrics:**

*Full points:* Correct and complete answer.

*Partial points:* Correct but not complete answer.

*No points:* No answer or Incorrect AND incomplete answers.

**Q1. [10 points]** What kind of information can you gather with Kali? List top five tools for security information gathering. <https://resources.infosecinstitute.com/topic/kali-linux-top-5-tools-for-information-gathering/>

Visit [www.netcraft.com](http://www.netcraft.com/) and do a search on at least three different websites of your choosing. Note/screenshot what information you can gather about each website. You can use Site Neighbours or Search DNS results.

**Q2. [10 points]** List (you can also make a table) top cybersecurity companies and their functions. <https://www.thesoftwarereport.com/the-top-25-cybersecurity-companies-of-2020/>

Select a local organization and conduct passive reconnaissance on it. This should include searching job boards, the organization’s own website, user groups/bulletin boards, social networking sites, [www.archive.org](http://www.archive.org/), and more. Gather as much information about the target network as you can.

**Q3. [10 points]** What do you mean by demystifying a keylogger? <https://home.sophos.com/en-us/security-news/2019/what-is-a-keylogger.aspx>

Note that this exercise may only be completed on machines where you have explicit permission to do so (not on public computers).

1. Using any website, find and download a key logger. The following websites might help you locate a key logger: [www.kmint21.com/familykeylogger/](http://www.kmint21.com/familykeylogger/) and [www.blazingtools.com/bpk.html](http://www.blazingtools.com/bpk.html) .
2. Install the key logger on your PC.
3. Examine how the key logger behaves on your machine. Do you notice anything that might indicate the presence of illicit software?
4. Run an antispyware software. Does the antispyware software detect the key logger?

**Q4. [10 points]** Google has uncovered espionage malware, which monitors and steals information about the target --including emails, messages and calls**.**  Using the Web, find and download a screen-capturing spyware application. <https://www.zdnet.com/article/this-android-spyware-can-record-calls-take-screenshots-and-video-targets-gmail-linkedin-snapchat/>

The following website might be helpful to you in selecting an appropriate product: <http://en.softonic.com/s/screen-capture-spy-software>. Warning: Since you are downloading spyware, it is likely that your system’s antivirus/antispyware will give you a warning.

1. Install and configure the application on your computer.
2. Run the application and note what it finds.
3. Run the antispyware and see whether it detects your spyware program.
4. Take screenshots and write ½ page critic on this software.

**Q5. [10 points]** How Does the Microsoft Firewall Work? Using Microsoft documentation, the Web, and other resources, find out what methodologies the Microsoft Windows (whichever version you are using) firewall uses. Write a brief essay explaining the strengths and weaknesses of that approach. Also discuss situations in which you feel that approach is adequate and those in which it might be inadequate.

**Q.6** **[10 points]** Briefly explain a Network Intrusion Detection & Prevention System. Go to the Snort.org website ([www.snort.org](http://www.snort.org/)) and download Snort. Using the vendor documentation or other resources, configure Snort. Then use port scanners on the machine that has Snort configured and note whether Snort detects the scan.

**Q7. [10 points]** What is IT/Cyber Disaster Recovery Plan? Using the knowledge you have gained far, create an IT disaster recovery plan for an organization. You may use a fictitious organization, but a real organization would be better. You may find the following resources helpful: www.cert.org www.sans.org

**Q8. [10 points]** What do you mean by the ethics of investigation?

Write an essay discussing the ethics of online investigations (e.g. finding phone numbers, criminal records, court cases etc.). Do you feel these investigations are an invasion of privacy? Why or why not? If you do feel they are an invasion of privacy, what do you think can be done about it? Are there problems with getting inaccurate information?

**Q9. [10 points]** What do you mean by computer forensics? OSForensics : Download a trial copy of OSForensics from <https://www.osforensics.com/osforensics.html>.

Using tutorials at <https://www.osforensics.com/faqs-and-tutorials/video_demonstrations.html>, perform basic forensics on your own computer with OSForensics.

**Q.10 [10 points]** Name some cybersecurity analysis and modeling tools. Consider the cybersecurity requirements of a college campus. Create a misuse-case diagram for a specific type of attack. Also, Create a requirements traceability matrix for penetration testing a campus computer network. You can choose any attack described in this book.